AU/ACSC/RATANAMALAYA, R/AY15

AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

Personal electronic devices and the ISR data explosion:

The impact of cyber cameras on the intelligence community

by

Richard S. Ratanamalaya, Civilian, NGA

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements for the Degree of

MASTER OF OPERATIONAL ARTS AND SCIENCES

Advisor: Mr. Michael P. Ivanovsky

Maxwell Air Force Base, Alabama

June 2015

Disclaimer

The views expressed in this academic research paper are those of the author(s) and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Abstract

How can the Intelligence Community (IC) utilize personal electronic devices, specifically cameras and posted images, for intelligence including access to denied areas; how feasible is this collection tool to operationalize; how do analysts analyze an overwhelming volume of data; and what are the implications legally and ethically? As new technology that allows the exploitation of personal electronic devices becomes more integrated into the IC, more powerful analytic tools must be developed to assist the intelligence analyst manage the overwhelming amount of data in order to provide any useful analytic value.

This paper will examine the intelligence value of wireless data sources and cyber cameras mounted on personal devices, security and maintenance systems, and photo trawling the internet. It will also look at the legal and ethical issues of employing such a collection strategy in the realm of national security then the feasibility of integrating and processing collected data into finished intelligence in an ever expanding world more data being collected than can be processed.

This paper is divided into three sections each focusing on technology and the problems associated with the exploitable nature of personal electronic devices, mainly devices with camera. The first section examines the domestic surveillance camera and privacy issues of electronic devices and technology within the realm of the criminal justice system in the United States. The second section examines how electronic devices can be utilized as covert collection platforms outside the United States to gather useful information for the intelligence community. The third section looks at the processing, exploitation, and dissemination problems the intelligence community faces with the vast amount of international information collected.

Essay

You are never alone in the surveillance state

The global arena has, for better or worse, become a surveillance state as public spaces are littered with surveillance cameras and individuals are consumed with personal electronic devices, most of which have embedded cameras. The number of security surveillance systems has increased primarily for criminal deterrence and to assist law enforcement and prosecutors. In addition, personal electronic devices such as cell phones, tablets, computers, and children's personal game systems have cameras. For example, in 2014 a suspected serial killer near the University of Virginia was imaged with an alleged victim on security cameras. The video of this man and woman together eventually led law enforcement to the identity and arrest of the alleged perpetrator. Another example would be the use of imagery collected by photographers and video cameramen to provide evidence of individuals committing crimes during riots and protests. Various forms of surveillance within the United States has proven valuable in the criminal justice system and has the potential to shape intelligence collection in a world where our adversaries employee similar internal surveillance and social media in their daily operations.

Utilizing surveillance technology in the international arena for intelligence collection has significant implications for US national security and may provide increased access for denied areas. The expansion of this technology to surveillance systems and personal electronic devices has potential to provide a treasure trove of information that may provide critical pieces to a complex intelligence puzzle. We already know open source media and photo trawling of the internet can provide valuable intelligence on weapon systems. For example, Chinese military enthusiast routinely post photos of new Chinese aircraft such as the J-20 and armored vehicles such as the ZBD-05 and ZLT-05 amphibious assault vehicles on websites such as Chinese Defense Mashup.[1] This type of open source information has provided the United States (US)

with valuable intelligence - but what if the Intelligence Community (IC) could take this technology to the next level and intercept surveillance video or manipulate personal electronic devices to collect camera photographs or digital video unbeknownst to the owner?

This paper will examine how the use of wireless data sources and cameras mounted on personal devices, security and maintenance systems, and photo trawling the internet can be utilized as passive collectors outside the US and the problems the IC faces dealing with the volume of data. Since this paper is primarily focused on the geospatial and imagery perspective for exploiting personal electronic devices, I will refer to the characteristics hereafter as cyber cameras when calling attention to their capabilities to be used as imagery collection platforms.

Section 1

Mobile device surveillance within the US criminal justice system

Surveillance cameras seem to be everywhere within the US recording government, commercial, and private spaces and events. In a large city such as New York, an individual is routinely imaged or recorded 73 to 75 times a day, according to a security camera industry estimate in 2000.[2] Assuredly, the imaging of an average person has increased over the decade since the September 11, 2001 terrorist attacks and other series of isolated terror and criminal events such as the Boston Marathon bombing. The presence of surveillance cameras in public areas has the potential to deter crime but criminals often move their activity to areas that are outside of the image window. [3] Traditionally, surveillance imagery was recorded over after a period of time; however, its historical value for discovery has been noted creating a secondary data storage problem.

Within the US, domestic surveillance is governed by the law and requires strict judicial justification and due process. Despite the proven value, statutes, as originally written, did not envision personal electronic devices such as cell phones, iPods, tablets, GPS, and numerous other applications.[4] Technology to collect data for use in criminal cases from personal electronic devices required a specialist to hack into the system and analyze data. Maureen Webb, in her book entitled **Illusions of Security: Global Surveillance and Democracy in the Post-9/11 World,** discussed the judicial and ethical decisions surrounding domestic surveillance. Her research details the legal limits of domestic intelligence and surveillance collection and offers a counter perspective to international surveillance issues. She notes that when all domestic legal documents are in order, it only takes a few keystrokes for a law enforcement official to begin collecting data on a target.[5]

A new twist on exploitation of personal electronic devices for law enforcement was derived from criminal activity itself. Aside from cybercrimes such as computer viruses and theft, criminals have hacked into computers and networks accessing information and photographs of individuals in order to blackmail or humiliate their victims. Recent examples include celebrity nude photographs and Sony internal email. Despite improvements in person electronic device security software, cyber cameras are so prevalent today, criminals are keen to take advantages of them to exploit individuals, businesses, and organizations. Regardless of the legal ramifications associated with invasion of privacy, criminals continue to counter security software and access private photographs and. Unfortunately, the potential exists to use cyber cameras on personal electronic devices to snoop on individuals wherever they are.[6] On January 12, 2015 the Twitter and YouTube pages of Central Command were hacked and modified to show Islamic State propaganda.[7] This example also shows how social media and systems can be attacked and used

as messaging for counter information operations could have been a commercial company or individual.

On the other end of the spectrum, law enforcement can utilize similar practices within the legal system. That said, there are severe domestic restrictions for law enforcement to conduct such activity. Conversely, commercial companies that produce and market personal electronic devices collect data on users for tailored advertising.[8] In many ways, much of the privacy individuals believe they have, has been forfeited willingly due to End User License Agreements (EULA) associated with personal electronic devices and software. This industrial trend is called Customer Relations Management (CRM). CRM services track individual user data, such as search engines and websites in order to provide tailored web advertising to an individual.[9] Network mapping such as that done with Twitter is another example. [10]

Section 2

Intelligence agencies collection restrictions

International data collection for the specific purpose of national security and intelligence is quite different from domestic surveillance. The ability to operate and collect data for intelligence purposes, as covered in Title 50 of the US Code, permits clandestine collection and identifies specific agencies to process and exploit foreign intelligence. The US Code also restricts intelligence agencies from conducting operations within the US. Intelligence operations within the US and against US persons or corporations are conducted by federal law enforcement agencies and not the subject of this section of the paper. For the purpose of this paper, surveillance in Sections 2 and 3 will focus on foreign intelligence collection in compliance with Title 50.

How mobile devices have changed the landscape of intelligence, surveillance, and reconnaissance for the IC

The concept of using cyber cameras or other personal mobile devices for intelligence has been discussed in depth by the authors C. Baber, C. Fulthorpe, and R. J. Houghton's article "Supporting Naturalistic Decision Making Through Location-Based Photography: A Study of Simulated Military Reconnaissance" in the **International Journal of Human-Computer Interaction**.[11] This article, as the authors noted, handled the sensitive nature of military ISR collection, processing, exploitation, and dissemination rather vaguely but effectively showed how cyber cameras and personal electronic devices equipped with GPS and metadata are a great advantage to military personnel in the field. For example photos taken by military intelligence personnel can be incorporated as a data later into analytic tools that map the location of enemy targets such as terrorist training camps or insurgent strong holds. The ability to overlay location, activity, and individuals, commonly referred to as human geography creates the ability to present a detailed representation of network that can be exploited or attacked. Link analysis, generated by programs such as Analyst Notebook, allows intelligence analysts to map out networks and identify critical notes. Once identified these critical nodes could permit direct military action or covert operations.

By applying a geospatial perspective, common to the management of international commercial communication networks, an intelligence analyst can develop a map of exploitable networks outside the US. The intelligence value of mapping this new digital data has been seen in commercial industries that mapped the urban landscape, commonly referred to as the new city landscape.[12] An example of this new city landscape can be seen with Twitter, a shared instant messaging system where users post messages and images on a public message board. Because

the software used by Twitter is sent on an open application programing interface (API), all messages can be collected to include additional data such as the GPS location it was posted from. This data can be used track individual users and map their location through time and space.[13] Although this data is similar to tracking normal communication data or signals intelligence (SIGINT) the combination of both cannot be overlooked. Identifying specific individuals or groups to follow and map, their respective network can provide significant intelligence value. The synergistic effect of combining geo-tagging of messages and photos, mapping the new urban landscape, will lead to the discovery of new intelligence targets to exploit and track for intelligence purposes. Despite the opportunities, the bigger problem now becomes the sheer volume of data created and filtering relevant intelligence in a timely and effective manner.[14]

What is gained from this ISR mission?

With simple technology, analysts can take numerous images from different sources, primarily cyber cameras, and create a mosaic of a denied area. Additionally, software exists that can remove people or objects from the image mosaic thus providing a clear picture of the scene or the people. Further, people of interest may be identified through facial recognition software. Internet searches with facial recognition software for selected individuals can build a pattern of life and a network of associates that can then be identified and mapped. After identifying individuals with intelligence value through social media, geo location, and social networking, intelligence officers could covertly manipulate their personal electronic devices to provide data such as imagery, voice, and location.

In the foreign intelligence realm, the ability to remotely turn on cyber cameras has great intelligence and surveillance potential. Hackers have already demonstrated this capability; however, when conducted for national security and intelligence collection, it can prove to be a

valuable tool. Imagine turning on a terrorist's cell phone camera. This data could provide real time location data as well as interior imagery of buildings that may provide Special Operations Forces (SOF) with floor plans before a raid. It also could provide access to other restricted areas, such as adversary nuclear research center or defense industry. Again, by simply identifying individuals based upon their intelligence value through social media, geo location, and social networking, their own personal electronic devices could be manipulated to provide data such as imagery, voice, and location data without the owner being knowledgeable.

Covertly manipulating cyber cameras could allow access to denied areas, most notably into buildings, where overt ISR methods, such a national systems, cannot collect. This can also provide ground truth into foreign government buildings and research facilities. For example, confirming suspicious activity related to weaponization inside an adversary nation's nuclear power plants or research site. Alternately, we could collect intelligence on individuals associated with locations of interest and use facial recognition to identify them. This could be done using security and maintenance cameras or open source information on the internet. Individual social networks can also be mapped and has potential for tracking other enemies of the state. When data is transmitted through wireless and other networks it can be intercepted. Restricted sites may ban cameras; however, they may have vulnerabilities because security and maintenance cameras are connected to the cyber domain and could be exploited. Of note, the cyber infrastructure or reliance on technology by a country may limit the ability to collect intelligence. For example, North Korea, with its limited cyber connectivity, may not be ideally suited for this method of collection.

Section 3

The problem of too much data and filtering intelligence value

Moore's law of computing capabilities, specifically its correlation to the Information Age where data increases exponentially, has created an immense volume of data that is too large to filter and analyze by human analysts. IBM's definition of this phenomenon, which is commonly referred to as "Big data," captures the problem.

> "Big data is being generated by everything around us at all times. Every digital process and social media exchange produces it. Systems, sensors and mobile devices transmit it. Big data is arriving from multiple sources at an alarming velocity, volume and variety. To extract meaningful value from big data, you need optimal processing power, analytics capabilities and skills."[15]

Big data was traditionally associated with textual or numerical data, but with the preponderance of cameras, digital imagery has become a significant percentage of all data stored. If not already, imagery data, will most likely account for the majority of data stored. For example, consider a cellphone and its large storage capacity, the majority of the data stored on it is likely images in the form of photographs or videos. In addition to personal data such as phone numbers, addresses, and account information stored physically on a phone, more individuals are storing data in the cloud. The cloud offers another layer of vulnerability as the devices must be networked which permits more opportunities to intercept or hack into data at the server.

Because there is so much data, the hardest part is to determine what is important and what is not. For an analyst in the IC, the sheer volume of information can be crippling because one independent piece of information could be the most important piece of a complex intelligence puzzle. Consequently, analysts need an information triage tool to sort and filter all

the intelligence data collected. Much of this can be accomplished through automated tools that can sift through the large volume of imagery, signals, and geospatial data using algorithms to tag data for the analyst to review.

Omerčević and Leonardis, in an article entitled "Hyperlinking reality via camera phones," provide a technical example of how cellphone camera photos can be hyperlinked to data. This software uses algorithms to search the internet for photos that were recently taken and registers them to a location through GPS in order to call out specific features such as building or restaurants. The program then provides that data back to the user on their cellphone using the original photos visually with hyperlinked data calling out features.[16] Technology such as this can be exploited for international intelligence collection if the cyber camera is remotely activated and imagery is clandestinely collected. This could be a primary tool for providing surveillance and intelligence of denied areas. Additionally, this technology could be used to assist intelligence analysts identify unknown areas depicted on an image. The ability to use these kinds of algorithms to match imagery data could more efficiently identify hostage locations or enemy encampments. Additionally, the same algorithms could be utilized by the IC to sort through collected imagery and provide only data on specific targets.

What can the IC do to best utilize the new technology landscape for ISR?

As new technology that allows the exploitation of personal electronic devices becomes integrated into the IC, more powerful analytic tools must be developed to assist the intelligence analyst manage the overwhelming amount of data. The devices ripe for imagery exploitation today include cell phones, security cameras, and web cameras. Additionally, social media and cloud storage offer opportunities for exploitation. When these mediums are integrated into the larger intelligence picture the US will have more opportunities to conduct intelligence operations

against our adversaries. These sources are readily available for exploitation because they are used around the world and openly broadcast through cell towers and Wi-Fi networks. The key technology required for exploitation will be cyber, electronic warfare, and signals based.

Regarding cost, because the technology taps into the adversary's personal electronic device or social media already connected to a network very little funding has to be spent on actual collections systems. The primary costs associated with this form of intelligence includes technology to hack into a personal electronic device; transmission and storage of data; analysts; and analytic tools.

Cyber vulnerabilities

Cyber security is critical to protecting industry, infrastructure, economy, and military power. It must be noted that all of the ISR methods discussed for exploitation of an adversary can be one's own vulnerability. The IC has to understand that cyber domain is highly contested and superiority within it is typically moments so any advantage the US may have in exploiting cyber camera or associated networks may be short lived. The fact of turning on cyber camera and intruding into data networks may also lead to tighter security measures like software or new systems that make it harder to exploit the vulnerabilities of this collection system.

Analytic tools and regulations required

New analytic tools and regulations must be developed to best utilize this cyber ISR strategy. Because this strategy relies so much on covert operations to turn on electronic devices in foreign nations it most likely would be associated with the IC; however, the military would also benefit from the strategy. The military would specifically be interested in weapons systems that are connected to the cyber network. This strategy is different from open source intelligence as it provides access to imagery and information unwittingly. To assist in this effort, software

and programs must be designed to assist analyst sort through the collected data. Much of this capability already exist such as motion detection algorithms that identify changes in the environment and facial recognition software.

Hard to exploit

This method of ISR is not suited for all targets due to their lack of reliance on technology. Nations or terrorist organizations may rely on modern cyber technology little to none making these targets hard to exploit. Just because personal electronic devices are prevalent and a nation is highly networked does not mean they are vulnerable. Due to the high profile nature of cybercrimes and awareness to remotely access personal electronic devices, developers have designed operating systems that mask data and use advanced encryption to provide enhanced security.

Conclusion

Technology such as cyber cameras and associated networks are so prevalent today they will eventually become ISR imagery collection platforms for the IC. These systems can provide unique ISR capabilities of denied areas that national systems cannot with minimal cost. The use of this collection system will overwhelm the intelligence analyst with big data and require new analytical tools to determine what information is useful. These tools may utilize powerful computer algorithms that key in on specific data sets and map networks for exploitation. Even though computers may eventually do the majority of the work, the analyst must remain in the loop to validate the information.

Bibliography

Books

Keenan, Kevin M., *Invasion of Privacy: A Reference Book*. Contemporary World Issues. Santa Barbara, CA: ABC-CLIO, Inc., 2005

Monmonier, Mark, *Spying with Maps: Surveillance Technology and the Future of Privacy* The Chicago, IL: University of Chicago Press, 2002.

Verton, Dan. *Black Ice: The Invisible Threat of Cyber-Terrorism* Emeryville, CA: McGraw Hill/Osborne, 2003.

Webb, Maureen. *Illusions of Security: Global Surveillance and Democracy in the Post-9/11 Word*, San Francisco, CA: City Lights Books. 2007.

Journals

Baber, C., C. Fulthorpe, and R. J. Houghton, "Supporting Naturalistic Decision Making Through Location-Based Photography: A Study of Simulated Military Reconnaissance." *International Journal of Human-Computer Interaction.* Vol. 26 Issue 2/3 (Feb/Mar 2010): 147-172

Neuhaus, Fabian. "New city landscape - Mapping urban Twitter usage." *Technoetic Arts: A Journal of Speculative Research.* Vol. 9 Issue 1 (2011): 31-48.

Omerčević, Dušan, and Aleš Leonardis, "Hyperlinking reality via camera phones." *Machine Vision & Applications.* Vol. 22 Issue 3 (May 2011): 521-534.

Online and Electronic Sources

China Defense Mashup website, http://www.china-defense-mashup.com/

IBM website, http://www.ibm.com/big-data/us/en/

Joseph Fitsanakis, "Research: Spies increasingly using Facebook, Twitter to gather data." *Intelnews.org*, 13 February 2012, http://intelnews.org/2012/02/13/01-927/?utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+intelNewsOrg+

Lamothe, Dan. "U.S. military social media accounts apparently hacked by Islamic State sympathizers," *Washington Post*, 12 Jan 2015. http://www.washingtonpost.com/news/checkpoint/wp/2015/01/12/centcom-twitter-account-apparently-hacked-by-islamic-state-sympathizers/

Mazmanian, Adam. "Surveillance disclosures haunt search for common ground on cybersecurity," *FCW: The Business of Federal Technology*, 28 Jan 2015. http://fcw.com/Articles/2015/01/28/Cybersecurity-common-ground.aspx?p=1

Texas Tech Security Group, "Automated Open Source Intelligence (OSINT) Using APIs." *RaiderSec*, Sunday 30 December 2012, http://raidersec.blogspot.com/2012/12/automated-open-source-intelligence.html

Endnotes

[1]*China Defense Mashup* website, http://www.china-defense-mashup.com/
[2] Kevin M. Keenan, *Invasion of Privacy: A Reference Book* (Santa Barbara, CA: ABC-CLIO Inc., 2005) 57.
[3] Ibid., 57.
[4] Dan Verton, *Black Ice: The Invisible Threat of Cyber-Terrorism* (Emeryville, CA: McGraw Hill/Osborne, 2003) 217.
[5] Maureen Webb, *Illusions of Security: Global Surveillance and Democracy in the Post-9/11 Word*, (San Francisco, CA: City Lights Books, 2007) 129-130.
[6] Adam Mazmanian, "Surveillance disclosures haunt search for common ground on cybersecurity," *FCW: The Business of Federal Technology*, 28 Jan 2015, http://fcw.com/Articles/2015/01/28/Cybersecurity-common-ground.aspx?p=1
[7] Dan Lamothe "U.S. military social media accounts apparently hacked by Islamic State sympathizers," *Washington Post*, 12 Jan 2015, http://www.washingtonpost.com/news/checkpoint/wp/2015/01/12/centcom-twitter-account-apparently-hacked-by-islamic-state-sympathizers/
[8] Mark Monmonier, *Spying with Maps: Surveillance Technology and the Future of Privacy* (Chicago, IL: The University of Chicago Press, 2002) 151-152.
[9] Kevin M. Keenan, *Invasion of Privacy: A Reference Book* (Santa Barbara, CA: ABC-CLIO Inc., 2005) 75-77.
[10] Fabian Neuhaus, "New city landscape - Mapping urban Twitter usage," *Technoetic Arts: A Journal of Speculative Research* Vol. 9 Issue 1 (2011) 31-48.
[11] C. Baber, Fulthorpe, C., and Houghton, R. J. , "Supporting Naturalistic Decision Making Through Location-Based Photography: A Study of Simulated Military Reconnaissance" *International Journal of Human-Computer Interaction.* Vol. 26 Issue 2/3 (Feb/Mar 2010) 147-172.
[12] Fabian Neuhaus, "New city landscape - Mapping urban Twitter usage," *Technoetic Arts: A Journal of Speculative Research* Vol. 9 Issue 1 (2011) 31-48.
[13] Texas Tech Security Group, "Automated Open Source Intelligence (OSINT) Using APIs," *RaiderSec*, Sunday 30 December 2012, http://raidersec.blogspot.com/2012/12/automated-open-source-intelligence.html
[14] Joseph Fitsanakis, "Research: Spies increasingly using Facebook, Twitter to gather data," *Intelnews.org*, 13 February 2012, http://intelnews.org/2012/02/13/01-927/?utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+intelNewsOrg+
[15] *IBM*, http://www.ibm.com/big-data/us/en/
[16] Dušan Omerčević and Leonardis, Aleš, "Hyperlinking reality via camera phones." *Machine Vision & Applications* Vol. 22 Issue 3 (May 2011) 521-534.